## IN THE CLAIMS

Please amend the claims as follows:

1. (Original) An implantable device comprising:

a receiver configured to receive data corresponding to a message and a first hash value generated as a function of the message;

a memory coupled to the receiver and configured to store a key and the message;

a hash value generator coupled to the memory and configured to generate a second hash value as a function of the key and the message; and

a comparator coupled to the hash value generator and configured to determine if the first hash value differs from the second hash value.

2. (Original) The device of claim 1 further including a clock configured to provide a time stamp to the memory and wherein the second hash value is generated as a function of the time stamp.

3. (Original) The device of claim 1 further including a number generator coupled to the memory and wherein the second hash value is generated as a function of a number provided by the number generator.

4. (Original) The device of claim 3 wherein the number generator includes at least one of any combination of a random number generator and a pseudo random number generator.

5. (Original) The device of claim 1 further including a key generator coupled to the memory and wherein the key is generated dynamically.

6. (Original) The device of claim 1 further including a therapy or monitoring circuit coupled to the receiver.

7. (Original) The device of claim 1 further including an inductive telemetry channel coupled to the memory.

8. (Original) The device of claim 1 wherein the hash value generator is configured to implement SHA-1.

9. (Original) The device of claim 1wherein the hash value generator includes a processor and executable instructions.

10. (Original) A method comprising:

receiving data at an implantable device, the data corresponding to a message and a first hash value generated as a function of the message;

storing a key and the message in a memory of the implantable device;

generating a second hash value as a function of the key and the message; and

comparing the first hash value and the second hash value.

11. (Original) The method of claim 10 further including storing a code in the memory and wherein the second hash value is generated as a function of the code.

12. (Original) The method of claim 11 wherein the code includes a time stamp.

13. (Original) The method of claim 10 wherein storing the key includes communicating with a near field communication link.

14. (Original) A device comprising:

a non-implantable transceiver configured to receive data from an implantable device corresponding to a message and a first hash value generated as a function of the message;

a memory coupled to the transceiver and configured to store a key and the message;

a hash value generator coupled to the memory and configured to generate a second hash

value as a function of the key and the message; and

a comparator coupled to the hash value generator and configured to determine if the first hash value differs from the second hash value.

15. (Original) The device of claim 14 wherein the transceiver includes a near field telemetry antenna configured to receive the key.

16. (Original) The device of claim 14 wherein the transceiver is configured for far field telemetry.

17. (Original) The device of claim 14 further including a code generator coupled to the transceiver, wherein the code generator provides a freshness code for a subsequent message.

18. (Original) The device of claim 17 wherein the code generator includes at least one of any combination of a clock and a random number generator.

19-24. (Canceled)

25. (Original) A system comprising:

an implantable device including:

a first far field transceiver;

a first processor coupled to the first far field transceiver; and

a first memory coupled to the first processor; and

an electrical circuit coupled to the processor; and

an external device including:

a second far field transceiver;

a second processor coupled to the second far field transceiver;

a second memory coupled to the second processor; and

a data port coupled to the second processor; and

wherein at least one of any combination of the first processor and second processor are

adapted to execute instructions to generate a first hash value based on a code generated by the first processor, a key stored in the first memory and the second memory and a message; and

wherein at least one of any combination of the first processor and second processor are adapted to execute instructions to generate a second hash value based on the message, the code and the key and adapted to compare the first hash value and the second hash value.

26. (Original) The system of claim 25 further including an inductive telemetry coil coupled to the first processor and adapted to communicate the key.

27. (Original) The system of claim 25 further including an inductive telemetry coil coupled to the second processor and adapted to communicate the key.

28. (Original) The system of claim 25 wherein the electrical circuit includes a therapy circuit.

29. (Original) The system of claim 25 wherein the electrical circuit includes a monitoring circuit.

30. (Original) The system of claim 25 wherein the data port includes at least one of any combination of a keyboard, a mouse, a controller, a data storage device, a network connection, a modem and a data bus.

31-46. (Canceled)

47. (Original) A method comprising:

receiving a code from a first device;

storing a key in the first device and in a second device, wherein at least one of the first device and the second device is implantable;

generating a first hash value at the second device, the first hash value generated as a function of the code, the key and a message;

receiving the message and the first hash value at the first device;

generating a second hash value at the first device, the second hash value generated as a

function of the code, the key and the message; and

comparing the first hash value and the second hash value at the first device.

48. (Original) The method of claim 47 wherein receiving the code includes a receiving a random number.

49. (Original) The method of claim 47 wherein receiving the code includes at least one of any combination of receiving a time stamp and generating a time stamp.

50. (Original) The method of claim 47 wherein storing the key includes generating a key.

51. (Original) The method of claim 50 wherein generating the key includes calculating a key as a function of stored data in the first device.

52. (Original) The method of claim 51 wherein calculating the key includes calculating a third hash value.

53. (Original) The method of claim 47 wherein storing the key in the first device includes communicating via an inductive coupling.

54. (Original) The method of claim 47 wherein storing the key in the second device includes communicating via an inductive coupling.

55. (Original) The method of claim 47 wherein storing the key includes encrypting the key.

56. (Original) The method of claim 47 wherein at least one of any combination of generating the first hash value and generating the second hash value includes executing a hashing algorithm.

57. (Original) The method of claim 56 wherein executing the hashing algorithm includes executing at least one of any combination of a secure hash standard algorithm and a message-digest algorithm.

58. (Original) The method of claim 57 wherein executing a secure hash standard algorithm includes executing at least one of any combination of SHA-1 and SHA-256.

59. (Original) The method of claim 57 wherein executing a message-digest algorithm includes executing at least one of any combination of MD2, MD4 and MD5.